Novel Method for Transmitting Robust Private Key Encryption Codes to Miniature Wireless Devices Such as Wireless Earbuds

02 July 2023
Simon Edwards
Research Acceleration Initiative

Introduction

The Bluetooth radio protocol has been in sore need of replacement since the day of its conception. Not only is this protocol prone to interference from other Bluetooth devices, the widespread use of this protocol has brought about an unseen but tangible cybersecurity crisis.

Given that this protocol does not employ encryption of any consequence, the door has been opened to operatives of foreign powers exploiting this security vulnerability. One need only to impersonate a pair of Bluetooth headphones in order to inject code into a device such as a smart phone that is actively exchanging data with those headphones. Although most of the data is flowing from smart phone to headphones, in order for Bluetooth to function, wireless communication transpires in both directions. In the event of a spoofing attack, a victim is likely only to experience an inexplicable loss of audio or attenuation of the bitrate of the audio being heard.

Although careful records are kept of Internet and cellular transmissions, low-power transmissions with a range of ~30 feet are not being, to the knowledge of this author, intercepted by, for example, American military intelligence. If they were, there is no possibility that the use of Bluetooth would have been permitted to endure for as long as it has given the number of breaches attributable to the PRoC into the personal devices via this vector.

Not only would an entirely overhauled short-range wireless protocol enhance our national security, it would likely be profitable. Once the security risks associated with Bluetooth become fully understood by the public, no company will remain profitable that does not phase out that protocol in favor of a new protocol based upon, perhaps, the forthcoming concept.

Abstract

512-bit encryption keys may be efficiently transferred to even those sorts of devices lacking keyboard inputs sc. wireless earbuds using low-frequency contact acoustics coupled with a microphone in the wireless earbuds. This should not increase the cost of manufacture of the earbuds as most already come equipped with microphones to support telephonic operations.

While high-frequency acoustic transmission of an encryption key runs the risk of acoustic intercept of a private key, an adversary would have a difficult time intercepting a key transmitted at a frequency that would be conducted

exclusively through the body of a smart phone and which would only be "heard" by an object touching the skin of the phone directly.

In some future scheme based upon this approach, a user might be prompted to bring both earbuds into contact with the phone so that its microphones may listen for sounds associated with this key transmission. While individual differences in phone composition and dimensions, protective cases used with smart phones and other factors such as whether the phone is on a table or being held in someone's hand would corrupt data encoded as variations to acoustic frequency, the precise duration of a series of pulses could be used to convey complex encryption keys. A pair of headphones that could distinguish between differences in pulse duration of 0.1ms, for example, could, within a few seconds, be programmed with a re-usable and secure key and would not require re-programming unless the phone's operating system were reinstalled or the phone was replaced.

This approach would be compatible with any headphone design and any smart phone design so long as the headphones each incorporate separate microphones and 0.1ms-timing pulse discrimination can be achieved, which it ostensibly can. One would need only to touch the earbuds to the front or back of a smart phone for a secure key to be transmitted in this manner.

Conclusion

512-bit encryption; even for casual applications such as music-listening; is essential given the ease with which foreign operatives may penetrate the devices of sensitively-placed individuals at public locales such as gyms, coffee shops, or with operatives even taking up residence in neighboring apartments in order to capture and inject wireless signals in the furtherance of their goals.

Extreme security measures taken within sensitive environments are in vain when one may safely infer that there is exists a high probability that any given individual in a public place living within a certain radius of known government facilities is in a position to interact with classified materials. By infecting devices en masse according to their area of usage (e.g. gyms in the Arlington, VA area,) an adversary could easily obtain classified information, personal information useful for the blackmail of government employees, or use bulk location data to identify clandestine satellite operations formerly unknown to the adversary.

In case there is any doubt of the reality of this style of attack, it is worth noting that the manufacturers of cellular devices that have, over the years, come into the Chinese sphere of influence have changed their security update policy to match the semi-annual schedule used by Motorola and other Chinese-owned manufacturers. Whereas a great deal of intelligence gathering depends upon the ability to penetrate cellular devices, regular security updates would pose a hindrance to such operations. Samsung's decision some time ago to switch to a semi-annual update schedule should be cause for grave concern.